

EXHIBIT “6A”

EXHIBIT “6A”

Las Vegas Metropolitan Police Department

Examination Report



Case Information

Event Number	210200075535
DFL Case Number	21-0300
Case Detective & P#	Detective A. Jacob, P# 14921
Exam Completion Date	March 4, 2021
Examiner Name & P#	Detective J. Rodriguez, P# 7191
Agency	Las Vegas Metropolitan Police Department
Description of Evidence	1. PK 1 IT 1- Red iPhone with an American Flag Cover 2. PK 2 IT 11- Silver Sony Digital Camera Ser# 783202 3. PK 4 IT 20- RCA Digital Recorder 4. PK 6 IT 49- Black Sony Digital Camera Ser# 613706 with Memory Card

Examination Report

Summary of Findings

I. Examiner Qualifications

I, Detective Johnny Rodriguez, P# 7191, with the Las Vegas Metropolitan Police Department, currently assigned as a forensic examiner at the Digital Forensics Lab, having been employed by the Department for over 19 ½ years.

I currently have more than 2,500 hours of police specific training, of which more than 390 hours are in areas relevant to conducting examinations on electronic storage devices and associated techniques. Please see the curriculum vitae that is located with the electronic report for further details.

II. Search Authorization

Authorization to search the electronic storage devices in reference to this case is granted by:

A search warrant authored by Detective A. Jacob, P# 14921, of the Las Vegas Metropolitan Police Department on February 24th, 2021.

Examination of the electronic storage device in this case is limited to searching for evidence of the crime(s) **Aggravated Stalking, Stalking with Use of Internet, Harassment (2 Counts), and Own/Possess Gun by Prohibited Person.**

III. Approved DFL Tools:

The following is a list of the specific tools used to image and examine the electronic storage device in this case:

- GrayKey v.1.6.10
- Cellebrite UFED4PC v. 7.42.0.18
- Cellebrite UFED Physical Analyzer v. 7.
- Cellebrite Multi SIM Adapter
- Ramsey STE3000F2 shielded test enclosure
- Cellebrite Memory Card Reader

IV. Evidence to be Examined:

The electronic storage devices consist of items in the custody of the Las Vegas Metropolitan Police Department, under LVMPD event number **210200075535**, Specifically, the items include the following:

1. PK 1 IT 1- Red iPhone with an American Flag Cover

Las Vegas Metropolitan Police Department Digital Forensics Lab Examination Report

- Device Make and Model: Apple iPhone XR (A1984)
 - IMEI: 356425107499898
 - Sprint SIM Card ICCID: 89312530000067318594
2. PK 2 IT 11- Silver Sony Digital Camera Ser# 783202
 - Device Make and Model: Sony Cybershot DSC-W100
 - Memory Card: Sony Memory Stick PRO-HG 8GB
 3. PK 4 IT 20- RCA Digital Recorder
 - Device Make and Model: RCA_Model NO: RP5032A
 4. PK 6 IT 49- Black Sony Digital Camera Ser# 613706 with Memory Card
 - Device Make and Model: Sony_Model NO: DSC-H3
 - Serial Number: 613706
 - Memory Card: SanDisk Memory Stick Pro Duo 1.0GB

I was assigned this case and retrieved the evidence package from the Digital Forensics Lab evidence vault and began my examination. The package contents were verified to include the search warrant and descriptions of the multiple devices. I read and verified the search warrant authorization for its search and seizure of the digital storage devices acquisition and data properties.

1. PK 1 IT 1- Red iPhone with American Flag Cover





On 03-02-21, a visual inspection of the mobile device was conducted. Digital Photos were taken. The device was placed inside the Ramsey STE3000F2 shielded test enclosure to block cellular connection and an attempt was made to turn on the device. The device battery was depleted and needed charging. I placed the device on a charger and extracted the SIM card. I identified the SIM card to be a Sprint SIM.

The device was charged and powered on. I placed the device in "Airplane Mode" and noticed the device did not have an activated security feature. I prepared the device for data acquisition.

I utilized GrayKey v1.6.10 for my device acquisition, which GrayKey was successful in obtaining a Full Filesystem extraction and generated a Full Filesystem SHA256 Hash of: a235045a69e4920329e6d45f8f6b9b55e4479daae84289c6b076ef29f07fc0a2.

GrayKey identified the following device properties:

Device Name: iPhone

Model: iPhone XR [iPhone11,8 N841AP]

IMEI: 356425107499898

Phone Number: 7023083378

Owner Name: Joshua Martinez

Accounts: [REDACTED]@yahoo.com, [REDACTED]@gmail.com, and [REDACTED]@gmail.com.

I utilized Cellebrite UFED 4PC v7.42.0.82 for my SIM card acquisition. I connected the SIM Card to the Cellebrite Multi SIM Adapter and performed a successful Advanced Logical extraction of the SIM Card.

All acquisitions were hashed utilizing Hasher. All data acquisitions were copied and titled "Data Copy", whereas, all copied acquisitions were hashed and saved.

All acquisitions for the mobile device were inputted into Cellebrite Physical Analyzer for analysis.

Cellebrite Physical Analyzer identified the following information from the mobile device acquisitions:

Detected Phone Model: iPhone XR

Serial: F2LZ2TQGKXKQ

IMEI: 356425107499898

IMEI2: 356425107074923

Last user ICCID: 89312530000067318594

MSISDN: 7023083378

Advertising Id (IDFA) #1: 9BAC4E7C-4BE7-4C9E-B84A-383E3B7BAD97

Apple ID: [REDACTED]@gmail.com

Time Zone: (UTC-08:00) Los_Angeles (America)

I did not perform further analysis for this device.

I generated a Cellebrite Extraction Report pdf file and generated a Cellebrite Reader file with the attached data downloads with the contents of the device.

2. PK 2 IT 11- Silver Sony Digital Camera



On 2-26-21, a visual inspection of the device was conducted. Digital Photos were taken. The memory card was removed from the device and photographed.

This device was given to Supervisor Z. Johnson, P# 8527, for the device acquisition. Supervisor Z. Johnson connected the device to his write blocker (Forensic Suites AFT EX-S3 MS reader) and utilized Magnet Acquire v. 2.31.0.22469 for the device acquisition and imaged the device into a (.EO1) file. Magnet Acquire generated a MD5 hash: 6d6bd989a0077b04532c9854e77dabcb, which was verified.

All data acquisitions were copied and titled "Data Copy". The "Data Copy" acquisition for the device was mounted in AccessData FTK Imager v.4.3.0.18, and the data was readily available to search the contents contained within the image file of the device.

On AccessData FTK Imager I located the file folder titled "DCIM". Found within this folder were .jpg images and another file folder titled "101MSDCF" with multiple videos and .jpg images.

I exported these files into the "Det Final Reports" file folder titled "Device Contents" which contain these located files from the image of the device. All exports were hashed with Hasher and saved within the file folder.

I did not locate any other files or folders found within the device contents.

3. PK 4 IT 20- RCA Digital Recorder



On 2-27-21, a visual inspection was conducted on the device. Digital photographs were taken.

I connected the device to a Tableau Forensic USB 3.0 Bridge (Write Blocker) and attached the write blocker to my forensic computer. I utilized AccessData FTK Imager 4.3.0.18 to create an E01 image of the device, which was successful.

AccessData FTK Imager identified the following device properties:

- Device Model: RCA_TKCF2494_US USB Device
- Drive Serial Number: 0xecc030008818b
- Serial Number: WD-WCC6Z5TFTCT7
- Source data size: 122 MB
- MD5 Hash: 3ab1fc4bf66a66ad4735d5054dfdafc1
- SHA1 Hash: dc71befaffb7bc3d39f3b3b7e803b39e98083f01

On AccessData FTK Imager I located the file folder titled "root". Found within this folder were folders titled "FOLDER_A through FOLDER_D, and MUSIC". Under the folder "FOLDER_A", there were 10 .mp3 files located within this folder. All other folders did not contain any files or folders for this device.

I exported these files into the "Det Final Reports" file folder titled "Device Contents" which contain these located files from the image of the device. All exports were hashed with Hasher and saved within the file folder.

I did not locate any other files or folders found within the device contents.

4. PK 6 IT 49- Black Sony Digital Camera Ser# 613706 with Memory Card





On 2-28-21, a visual inspection was conducted on the device. Digital photographs were taken.

I connected the device to my forensic computer Forensic Suites AFT EX-S3 MS/DUO- (Write Blocker) and verified write blocked. I utilized AccessData FTK Imager 4.3.0.18 to create an E01 image of the device, which was successful.

AccessData FTK Imager identified the following device properties:

- Device Model: RCA_TKCF2494_US USB Device
- Drive Serial Number: 000000000575
- Source data size: 951 MB
- MD5 Hash: 77c21a14ec966786f2fdc21e6bb4003b
- SHA1 Hash: 3b46b9ff1b124856631a3370a29cf9682e9fdd1b

On AccessData FTK Imager I located the file folder titled "DCIM". Found within this folder were .jpg images and another file folder titled "101MSDCF" with multiple videos and .jpg images.

I exported these files into the "Det Final Reports" file folder titled "Device Contents" which contain these located files from the image of the device. All exports were hashed with Hasher and saved within the file folder.

I did not locate any other files or folders found within the device contents.

V. Additional Information

Case investigators/ detectives need to review all reports and bookmarks for relevancy and compliance with the search warrant.

A copy of my Curriculum Vitae (CV) listing training and certifications I have received in the field of digital forensics can be found on the provided media.

The devices were impounded back into the LMVPD Evidence Vault.

The attached reports and files include findings based on a Forensic Exam performed on the listed digital devices.

END OF REPORT.

Signature Detective J. Rodriguez, P# 7191 Date 03/04/2021